

March 24, 2009

Control Number: OSPIPDS-10-0309-01

MEMORANDUM FOR DISTRIBUTION

FROM: Deborah Wolf /s/ Debra Diener, Acting
Director, Privacy, Information Protection and Data Security

SUBJECT: Interim Guidance – Reporting Losses, Thefts and
Disclosures of Sensitive Information

When sensitive information is lost, stolen, or inadvertently disclosed in any way, whether it be electronically, verbally or in hardcopy form, employees are currently required to report the incident to their manager, CSIRC and TIGTA within one hour of becoming aware of the incident.

In an effort to lessen the reporting burden on employees, simplify the incident reporting process, and minimize duplication of efforts, the Computer Security Incident Response Center (CSIRC) incident reporting form has been redesigned to account for all losses, thefts and disclosures of sensitive information. Business unit representatives were consulted as the form was redesigned.

The changes that will impact the current process include the following:

- Form 10848, Report of Unauthorized Inadvertent Disclosure of Tax or Privacy Act Information, is obsolete effective with the receipt of this memorandum and will no longer be used for reporting disclosure incidents.
- The CSIRC incident reporting form should be used by all employees for reporting losses, thefts and disclosures of sensitive information. The [Computer Security Incident Reporting Form](#) is designed to be used online. Several questions were added to the incident reporting form and some existing questions were modified to improve clarity.
- Disclosure incidents (inadvertent disclosures) will no longer be reported to TIGTA as part of this process.
- An exception to the normal reporting requirements is made for disclosure incidents involving a potential erroneous notice issuance. Employees who learn of such an incident will not be required to notify CSIRC. The employee will follow existing procedures in [IRM 21.3.1.1.1](#) to notify the Notice Gatekeeper, who will notify CSIRC as necessary after an initial analysis of the incident. This procedure minimizes the potential for inaccurate, incomplete, and duplicate reporting of incidents to CSIRC, lessens the operational impact of reporting an incident, and focuses resources on correcting the error to prevent additional breaches.

Under the new guidelines, upon becoming aware of a loss, theft or disclosure of sensitive information, you are required to report the incident within one hour to:

- Your manager
- The Computer Security Incident Response Center (CSIRC) [online](#), or call (866) 216-4809
- If the incident involves the loss or theft of an IT asset or hardcopy data, TIGTA at (800) 366-4484

An exception is made in the case of a potential erroneous notice issuance, which should be reported to the Notice Gatekeeper [online](#) through the Servicewide Notice Information Program (SNIP) Web site.

If you see indications of a voluntary and intentional unauthorized disclosure, the incident must be reported to TIGTA. See [IRM 11.3.1.6:\(2\)](#) and [IRM 11.3.38.6:\(1\)](#).

Check the [Operation R.E.D.](#) page on IRWeb for more information on existing policies and procedures about encrypting, safeguarding and protecting sensitive information, including personally identifiable information (PII).

Internal Revenue Manual (IRM) 10.5.3 *Identity Theft and Incident Management Program*, is currently being updated. Due to the time it will take to make those updates, the procedures described in this memorandum will act as interim guidance for the IRS and take effect immediately. The procedures will be available on IRWeb and will be included in a SERP Alert.

1. Source of Authority: IRM 10.5.3 is issued in support of OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007.

2. Effect on other Documents:

IRM 10.8.1, *Information Technology Security Policy and Guidance*

IRM 11.3.1.6 *Reporting Unauthorized Accesses or Disclosures*

IRM 11.3.38.6.1, *Report of Inadvertent Improper Disclosures*

IRM 3.12.279.30, *Erroneous Notice Procedures*

IRM 21.3.1.1.1, *Erroneous Notice Procedures*

3. Contact: If you have any questions about this guidance, please contact Kyle Ballew, Program Manager, Incident Management, at (202) 283-6867, or Mike LaMothe at (202) 927-0748.

4. Expiration Date: This guidance will be incorporated into IRM 10.5.3 by March 24, 2010.

Distribution

Chief of Staff, Office of the Commissioner

Deputy Commissioner for Operations Support

Deputy Commissioner for Services and Enforcement
Commissioner, Large and Mid-Size Business Division
Commissioner, Small Business/Self-Employed Division
Commissioner, Tax Exempt and Government Entities Division
Commissioner, Wage and Investment Division
Chief, Agency-Wide Shared Services
Chief, Appeals
Chief, Communications and Liaison
Chief Counsel
Chief, Criminal Investigation
Chief, Equal Employment Opportunity and Diversity
Chief Financial Officer
Chief Human Capital Officer
Chief Information Officer
Director, Office of Professional Responsibility
Director, Research, Analysis & Statistics
National Taxpayer Advocate

cc:

Office of Disclosure
Office of Cybersecurity Policy and Programs
Office of Cybersecurity Operations
Office of Electronic Services and Programs
Office of Service-wide Policy, Directives & Electronic Research
<http://www.irs.gov>